Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE



# PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 39778/S850

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on December 20, 2005

Signature: /Christina L. Vann/

Typed or printed name: Christina L. Vann

| Application Number | Filed |
|---|---|
| 09/688,456 | 10/16/2000 |

First Named Inventor: Craig L. Ogg

| Art Unit | Examiner |
|---|---|
| 3621 | Firmin Backer |

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [X] attorney or agent of record. Registration number 43,945
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/Raymond R. Tabandeh/
Signature

Raymond R. Tabandeh
Typed or printed name

626-795-9900
Telephone number

December 20, 2005
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of _____ forms are submitted.

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

*I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 20, 2005.*

Christina L. Vann

| | | |
|---|---|---|
| Applicant | : Craig L. Ogg, et al. | Confirmation No. 1637 |
| Application No. | : 09/688,456 | |
| Filed | : October 16, 2000 | |
| Title | : CRYPTOGRAPHIC MODULE FOR SECURE PROCESSING OF VALUE-BEARING ITEMS | |
| Grp./Div. | : 3621 | |
| Examiner | : Firmin Backer | |
| Docket No. | : 39778/S850 | |

**REMARKS FOR PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Post Office Box 7068
Pasadena, CA 91109-7068
December 20, 2005

Commissioner:

Claims 1-71 are pending in this application. In the Final Office action of September 23, 2005, Applicant's arguments with respect to claims 1-71 were considered moot in view of the new ground(s) of rejection. Claims 1-71 are now rejected under 35 U.S.C. 102 (e) as being clearly anticipated by Lewis et al., U.S. 6,223,565 ("Lewis").

To establish a *prima facie* case of anticipation, the Examiner must establish that the cited reference teach every aspect of the claimed invention either explicitly or impliedly. In regard to claim 1, this claim includes the elements of "A cryptographic system for securing data on a computer network comprising: a plurality of users coupled to the computer network; and a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising: a processor programmed to authenticate the plurality of remote users on the computer network for secure processing of a value bearing item (VBI); a memory for storing security device transaction data

for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users; a cryptographic engine for cryptographically protecting data; an interface for communicating with the computer network, and a module for processing value for the value bearing item, wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users, wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users, and wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users." Appellant believes that the Patent Office has failed to establish that the cited reference teaches each of these elements of claim 1 and therefore has failed to establish a *prima facie* case of anticipation for claim 1.

In regard to the element of "a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users," the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of users. Rather, Lewis describes a single cryptographic module (14) that is remote from the users. As illustrated in FIG. 1, Lewis discloses a remote service provider (RSP) 4, and a third party seller of goods and/or services (TPS) 6... . The client 2n has a Host system 10n and a PSD 20n which is resident on a [single] server of RSP 4. The Host 10n accesses the remote PSD 20n via the Internet 30." (Col. 6. lines 39-59, emphasis added). The single server 4 comprises of its own single cryptographic module 14. (Col. 21, lines 64-65, emphasis added). Lewis further describes that each client 2n has its own cryptographic module 12. However, these client cryptographic modules 12 are not each "remote from the plurality of users." That is, at least one of the client cryptographic modules 12 is local to at least one user.

Regarding the element of "a module for processing value for the value bearing item," Lewis does not teach this element. Rather, in the system of Lewis, a Transaction Manager server 180 processes the value for all of the client transactions. See, for example, Col. 25, lines 5 -1, emphasizing that "once the client 2 has been authenticated, it submits a transaction request to the transaction server 180 and waits for a response. It now becomes the job of the Transaction Manager to process the transaction and return a "receipt" to the client 2. All transaction

"receipts" will contain a date/time stamp, and a sequence number and a digital signature to verify the authenticity of a transaction . . .." Therefore, "processing value" in Lewis is performed by the transaction server 180 and not by a module in each of a plurality of cryptographic devices.

Regarding the claimed element "wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users," Lewis fails to teach this element. First, as mentioned above, the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the plurality of users, there is no description in Lewis that each of these imaginary server cryptographic devices is capable of authenticating any of the plurality of remote users. In fact, Lewis specifically describes that the cryptographic module 14 stores the Client Public Authentication Keys, which are used to prove the client's identity (that is, to authenticate the client), when a client attempts to establish a connection with the server 4. (Col 25, line 63-67. Also, see, Table III at the end of Col. 27, and col. 27, lines 58-59.).

Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able to authenticate any of the plurality of users, because each cryptographic device would have had to maintain and update the Public Authentication Keys for all of the clients. There is no teaching in Lewis about this. Furthermore, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device, meaning that a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package." (Specification, page 8, lines 13-16). Moreover, a PSD package for each of the imaginary server cryptographic devices would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Id., lines 22-24). There is no teaching in Lewis about this either.

Regarding the element "wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users," Lewis does not disclose this element. First, as mentioned above, the system of Lewis dose not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a

plurality of server cryptographic devices remote from the users, there is no description in Lewis that each of these server cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users.

Regarding the claimed element "wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users," Lewis falls short of teaching this element. First, as mentioned above, the system of Lewis does not have a plurality of cryptographic devices remote from the plurality of users. Second, even if Lewis described a plurality of server cryptographic devices remote from the users, there is no description in Lewis that each of these server cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.

Indeed, Lewis specifically describes that the cryptographic module 14 maintains the Client Private Indicium Keys, which are used to generating indicia data for that client. (Table III at the beginning of col. 28). Therefore, even if Lewis had a plurality of server cryptographic devices remote from the users, each of those devices would not have been able generate indicia data for transmitting to any of the plurality of users, because each cryptographic device would have had to maintain and update the Client Private Indicium Keys for all of the clients. There is no disclosure in Lewis about this.

Moreover, Lewis describes that "the first step to indicium generation is generating a public/private key pair for the server 4 [cryptographic module 14]. The public key is sent to the Certification Authority and a certificate for that server 4 is generated and returned to the Server. The Certification Authority also retains this certificate so that the Certification Authority can verify the authenticity of future server requests. Similarly, the server 4 will have a copy of the CA's certificate to verify the authenticity of data being sent back from the CA." (Col. 30, line 63 to col. 31, line 4). Consequently, the Certification Authority would have had to retain a different certificate for each of the imaginary server cryptographic devices to verify the authenticity of future server requests. There is no teaching in Lewis about this either.

Finally, each of the imaginary server cryptographic devices of Lewis would have had to be "stateless device and a PSD package for each of the imaginary server cryptographic devices

would have had to include "all data needed to restore the PSD to its last known state when it is next loaded into a [different] cryptographic module." (Specification, page 8, lines 13-24). There is no teaching in Lewis about this either.

As a result, the Patent Office has failed to establish that the cited reference teaches each of the elements of claim 1 and therefore has failed to establish a *prima facie* case of anticipation for claim 1.

Claim 41 includes similar limitations as the limitations of claim 1, therefore, a *prima facie* case of anticipation for claim 41 is also not established.

Accordingly, it is submitted that the rejections of claims 1 and 41, and their respective dependent claims based on 35 U.S.C. § 103 be overturned.

CLV PAS658412.1-*-12/20/05 5:10 PM